Köln, 21 July 2020

ECJ declares basis for data export to the USA ineffective

#Data protection in the EU (GDPR); #EU-US Privacy Shield ineffective; #Standard contract clauses remain valid; #Additional measures;

The European Court of Justice (ECJ, Case C-311/18)) has declared the EU-US agreement on the so-called Privacy Shield invalid. This agreement regulates the conditions for ensuring that the transfer of personal data of EU citizens or residents to the USA meets the requirements of the European Data Protection Regulation (DSGVO). To this end, US companies must be certified accordingly as recipients of the protected data. As a consequence of the ECJ ruling, the transfer of personal data to the USA lacks its essential legal basis. The ECJ justifies its view with the inadequate protective measures and legal protection options contained in the Privacy Shield. In particular, this is due to the electronic surveillance measures against foreigners carried out abroad as permitted under US law. The decision was based on procedures initiated by data protection activist Max Schrems against the Irish Date Protection Commissioner. Schrems had lodged a complaint against the transfer of his personal data by Facebook Ireland to its US parent company, Facebook, Inc..

There is another legal basis for data transfer to the USA, namely the so-called standard contractual clauses. These model clauses are considered by the European Commission (the Executive Body of the European Union) to be appropriate for agreements relating to the export of data. In particular, the standard contractual clauses are agreed with data importers established in third countries which do not provide for data protection in line with EU law. Only 12 countries are currently regarded as so-called safe third countries, whose data protection therefore meets EU standards without further measures. The USA has not been a safe third country either. Safe Harbour and, from 2016, Privacy Shield were only intergovernmental agreements to bring data protection in the USA into line with the status of a safe third country in relations between parties to these agreements.

In the new decision, the ECJ also comments on the standard contractual clauses. These were included in the agreement between Facebook and Max Schrems. However, they only have an effect in the relationship between the parties to the contract and do not bind the authorities concerned. Among other things, they contain detailed provisions on information that the data importer must provide to the exporter (e.g. on potential government interference) and on the liability of the parties. In principle, the parties must examine the extent of data protection in the importing country. However, the supervisory authorities can also intervene and, if necessary, prohibit the transfer of data.

Depending on the form of data protection in the recipient country, the ECJ considers that additional measures must be taken to bring data protection in the importing country into line with EU standards. Unfortunately, the court does not explain what specifically needs to be done with regard to the USA. In its most recent ruling, the ECJ considered monitoring measures by the US authorities on foreigners to be particularly problematic. It is true that the standard contractual clauses in the agreement between the parties can be supplemented by additional obligations to provide information in the event of control measures by state authorities, provided the importer of the data becomes aware of them. Such cases can then entitle to terminating the contract or to cancelling the data transfer. However, this does not change the fundamental problem. This consists of the fact that, from the EU point of view, unauthorised interference with data protection can occur, e.g. through surveillance measures. In most cases these cannot be foreseen in advance by the parties to the data transfer agreement.

Only a new agreement between the EU and the US, which takes into account the reservations of the ECJ, can provide a lasting remedy. However, the Commission also intends to present a revision of the standard contract clauses shortly. This should provide clearer guidance to the parties on the aspects which the ECJ has identified as critical.

For cross-border data transfers that take place within groups of companies, binding corporate rules can be considered as a basis of legitimacy. These must be approved in advance by the competent data protection authority. They then form the basis for a lawful data transfer to a non-secure third country. The ECJ ruling does not call into question the validity of such rules.

It is strongly recommended that, as a consequence of this ECJ ruling, companies centrally record and verify all transfers of personal data to non-EEA and non-secure third countries. The limitations expressed by the ECJ on the validity of standard contractual clauses are likely to have implications beyond the specific reference to data transfers to the US. According to the ECJ ruling, the parties to a cross-border data transfer agreement (i.e. both exporter and importer) are obliged to examine whether the obligations and guarantees regulated in the standard contractual clauses are sufficient in the specific case to bring data protection under the law of the recipient of the data into line with EU standards.

Encrypted transmission of data is also possible. However, this form of transfer is not as reliable as one might initially assume. In many cases, the decryption key can be accessed by the supervisory authorities.

This review of the concrete impact of the data protection law of the recipient country to be performed by the entity intending to transfer personal data to non-secure third countries should clarify the following questions:

1) To which relevant countries does the company transfer personal data, i.e. to countries outside the EEA that are not safe third countries?

2) For what reasons can the authorities gain access to relevant personal data under the laws of the data importing country? If the authorities are formally entitled to control personal data for reasons other than the protection of public security, prevention and prosecution

of criminal offences, the parties have to define additional safeguards in order to achieve a level of data protection comparable to the EU standard. In this context, the ECJ refers to Section 702 FISA (Federal Law on Interception of Intelligence Services, entered into force in 2008) as a provision which gives rise to the assessment that the level of data protection in the US is below EU standards. Section 702 allows the US federal government to carry out targeted surveillance of foreign persons outside the USA. In doing so, the assistance of providers of electronic communications services can be forced in order to obtain foreign intelligence information. The above legal basis is further strengthened by Executive Order 1233 of 1981, which addressed the same subject and was made on the basis of a predecessor provision to Sec. 702.

For data transfer with the USA, in the wake of the ECJ there is considerable uncertainty until a new agreement is concluded to replace the Privacy Shield. However, the EU and the US authorities are already expected to be coordinating their efforts in that direction.

Please contact us if you have any questions:

Dr. Hermann Knott, LL.M. (UPenn)
Rechtsanwalt, Attorney-at-Law (New York) / Partner

Andersen Rechtsanwaltsgesellschaft Steuerberatungsgesellschaft mbH
Gustav-Heinemann-Ufer 74
50968 Köln
Germany
hermann.knott@de.Andersen.com
Tel: +49 221 88835 502

Dr. Fritjof Börner
Rechtsanwalt / Of Counsel

Andersen Rechtsanwaltsgesellschaft Steuerberatungsgesellschaft mbH
Ulmenstraße 22
60325 Frankfurt am Main
Germany
fritjof.boerner@de.Andersen.com
Tel: (+49) 69 979953 0